RECORD AND BRIEFS

FILED
AUG 28 2017
OFFICE OF THE CLERK

No. 17-2

IN THE

Supreme Court of the United States

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION

UNITED STATES OF AMERICA,

Petitioner,

v.

MICROSOFT CORPORATION,

Respondent.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

BRIEF IN OPPOSITION

Bradford L. Smith
David M. Howard
John Frank
Jonathan Palmer
Nathaniel Jones
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052

James M. Garland
Alexander A. Berengaut
COVINGTON & BURLING LLP
850 10th Street, NW
Washington, DC 20001

E. Joshua Rosenkranz
Counsel of Record
Robert M. Loeb
Brian P. Goldman
Evan M. Rose
Hannah Garden-Monheit
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019
(212) 506-5000
jrosenkranz@orrick.com

Counsel for Respondent

RECORD AND BRIEF

AUG 28 2017

No. 17-2

IN THE

Supreme Court of the United States

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION

UNITED STATES OF AMERICA,

Petitioner,

v.

MICROSOFT CORPORATION,

Respondent.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

BRIEF IN OPPOSITION

Bradford L. Smith
David M. Howard
John Frank
Jonathan Palmer
Nathaniel Jones
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052

James M. Garland
Alexander A. Berengaut
COVINGTON & BURLING LLP
850 10th Street, NW
Washington, DC 20001

E. Joshua Rosenkranz
Counsel of Record
Robert M. Loeb
Brian P. Goldman
Evan M. Rose
Hannah Garden-Monheit
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019
(212) 506-5000
jrosenkranz@orrick.com

Counsel for Respondent

Library of Congress
Law Library

QUESTION PRESENTED

The Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, part of the Electronic Communications Privacy Act of 1986, protects the privacy of communications in electronic storage. It restricts hackers from "access[ing]" stored electronic communications (§ 2701) and bars providers of electronic communications services from voluntarily "divulg[ing]" the contents of stored communications without permission of the customer (§ 2702). The Act also creates a limited exception to the prohibitions on accessing and divulging the contents of communications in electronic storage. Under that exception, a federal, state, or local law-enforcement officer may obtain a search warrant to compel a service provider to access and disclose the content of stored electronic communications (§ 2703).

The question presented is:

Given the presumption against applying federal law in other countries and the Government's concession that Congress did not intend to apply the Stored Communications Act outside the United States, are private electronic communications stored in Ireland outside the scope of the Stored Communications Act's interlocking provisions?

CORPORATE DISCLOSURE STATEMENT

Microsoft Corporation, a publicly traded company, has no corporate parent, and no publicly held company has an ownership interest of more than ten percent.

TABLE OF CONTENTS

Page

QUESTION PRESENTED i

CORPORATE DISCLOSURE STATEMENT ii

TABLE OF AUTHORITIES iv

INTRODUCTION 1

STATEMENT 7

REASONS FOR DENYING CERTIORARI 13

I. Further Review Is Not Warranted Because Congress Is Actively Considering Amendments To The SCA That Would Expressly Provide For Limited Extra-territorial Reach. 14

II. The Court Of Appeals' Decision Is Correct And Fully Consistent With This Court's Extraterritoriality Precedents. 26

III. Because This Is A Question Of First Impression In The Courts Of Appeals, This Court Should Await Further Percolation. 35

CONCLUSION 37

TABLE OF AUTHORITIES

Page(s)

Cases

Benz v. Compania Naviera Hidalgo, S.A., 353 U.S. 138 (1957) 3

EEOC v. Arabian Am. Oil Co., 499 U.S. 244 (1991) 12, 14

F. Hoffmann-La Roche Ltd. v. Empagran S.A., 542 U.S. 155 (2004) 4, 16

In re Google Inc. Cookie Placement Consumer Privacy Litig., 806 F.3d 125 (3d Cir. 2015) 27

Kiobel v. Royal Dutch Petroleum Co., 133 S. Ct. 1659 (2013) 4, 25

Marc Rich & Co., A.G. v. United States, 707 F.2d 663 (2d Cir. 1983) 33

Maslenjak v. United States, 137 S. Ct. 1918 (2017) 35

Mohamad v. Palestinian Auth., 132 S. Ct. 1702 (2012) 33

Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247 (2010) 10, 11, 22, 27, 30, 34

Riley v. California,
134 S. Ct. 2473 (2014).....8

RJR Nabisco, Inc. v. European Cmty.,
136 S. Ct. 2090 (2016).....2, 26, 30

In re Search of Content Stored at Premises Controlled by Google Inc.,
No. 16-MC-80263, 2017 WL 3478809
(N.D. Cal. Aug. 14, 2017).....35

In re Search of Info. Associated with [redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc.,
No. 16-MJ-00757, 2017 WL 3445634
(D.D.C. July 31, 2017) 23

In re Search Warrant No. 16–960–M–01 to Google, No. 16-1061-M,
2017 WL 471564 (E.D. Pa. Feb. 3,
2017).....35, 36

In re Search Warrant No. 16-960-M-01 to Google,
232 F. Supp. 3d 708 (E.D. Pa. 2017) 23

Theofel v. Farey-Jones,
359 F.3d 1066 (9th Cir. 2004).....27

Statutes

Electronic Communications Privacy Act, 18 U.S.C. § 2701, *et seq.*

18 U.S.C. § 2701.....6, 7, 27, 28, 29

18 U.S.C. § 2701(c)(3) 8, 28

18 U.S.C. § 2702.....6, 7, 28, 29

18 U.S.C. § 2702(b)(2).....8, 28

18 U.S.C. § 2703.....6, 7, 8, 12, 28, 29, 30, 31, 33

18 U.S.C. § 2703(a) 9, 18, 28

18 U.S.C. § 2703(g) 32

18 U.S.C. § 2711(4) 8

Legislative Materials

Email Privacy Act, H.R. 387, 115th Cong. (2017) 18

European Union's General Data Protection Regulation.....17

H.R. Rep. No. 99-647 (1986) 7

International Communications Privacy Act, S. 1671, 115th Cong. (2017).....15, 20, 21

S. Rep. No. 99-541 (1986).....7

Other Authorities

Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights: Hearing Before the S. Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary, https://perma.cc/GB66-6CTS 16, 19, 21

Letter from industry groups to Sens. Orrin Hatch and Christopher Coons (July 27, 2017), https://perma.cc/6482-3Z93 21

Letter from Samuel R. Ramer, Acting Assistant Att'y Gen., Office of Legislative Affairs, U.S. Dep't of Justice, to Hon. Paul Ryan, Speaker, U.S. House of Representatives (May 24, 2017), https://perma.cc/MUT6-A8GC 1

Letter from technology companies to Sens. Orrin Hatch, Christopher Coons, and Dean Heller, https://perma.cc/KCN9-XJ64 21

Press Release, Second Circuit Ruling Gives Data Privacy Bill Momentum in Congress (July 14, 2016), https://perma.cc/BF49-N2YE 19

Press Release, Sen. Orrin Hatch, Hatch Statement on DOJ Decision to Seek Review in Microsoft Warrant Case (June 26, 2017), https://perma.cc/QRG4-4NBH 21

Press Release, Sen. Orrin Hatch, Hatch Urges Senators to Support International Communications Privacy Act (Aug. 1, 2017), https://perma.cc/96FP-PXDY.....18

U.S. Dep't of Justice, Office of Justice Programs, Bureau of Justice Assistance, *Electronic Communications Privacy Act of 1986*, Justice Information Sharing, https://perma.cc/S5NA-WZTB 27

INTRODUCTION

The Government concedes that when Congress enacted the Stored Communications Act (SCA) in 1986, it said absolutely nothing about applying the Act to reach communications stored overseas. Congress did not focus on—and could scarcely have imagined—a world where a technician in Redmond, Washington, could access a customer's private emails stored clear across the globe. Yet the Government asks this Court to extend the SCA to private emails stored in Ireland. The Government is in the wrong forum.

The Government has itself acknowledged that Congress is the branch that should address how to modernize the SCA. Less than a month before filing its petition for certiorari, the Department of Justice sent a letter to the Speaker of the House, the President of the Senate, and the Chairmen and Ranking Members of the House and Senate Committees on the Judiciary, proposing legislation to update the statute in light of the Second Circuit's ruling to address the novel phenomenon of "cross-border electronic data."[1] The Government was right to appeal to Congress for the same reason it is wrong to ask this Court to intervene now: Under this Court's settled extraterritoriality doctrine, revising a federal statute to account for

---

[1] Letter from Samuel R. Ramer, Acting Assistant Att'y General, Office of Legislative Affairs, U.S. Dep't of Justice, to Hon. Paul Ryan, Speaker, U.S House of Representatives at A-1 (May 24, 2017), https://perma.cc/MUT6-A8GC.

the globalization of data is a job for Congress, not courts.

Given the consensus that Congress expressed no intent to apply the SCA's provisions in foreign countries, the Second Circuit correctly held that the Government has no authority under current law to order Microsoft to "collect, import, and produce to the government customer content stored outside the United States." Pet. App. 5a. The Government argued that such a power would make good policy. But the court understood that its job was not to speculate "whether ... Congress 'would have wanted' the statute to apply extraterritorially had it foreseen the precise situation" now presented, Pet. App. 57a (Lynch, J., concurring) (quoting *RJR Nabisco, Inc. v. European Cmty.*, 136 S. Ct. 2090, 2100 (2016)).

That is not to say the statute is fine as is. Everyone agrees that there is a clear "need for congressional action" to update the statute to address the worldwide mobility of data. Pet. App. 49a (Lynch, J., concurring). When Congress acts, it will do so on the basis of complete information and with a wide range of remedial options. It will doubtless weigh heavily the needs of federal, state, and local law enforcement. But it will also weigh other considerations, such as: the interest in maintaining protections commensurate with the public's privacy expectations for our most personal communications and documents; the dangers of infringing foreign sovereignty by unilaterally seizing personal communications data from a foreign country, potentially in violation of foreign law; and the adverse effects the U.S. technology sector will suffer if it

becomes the conduit through which U.S. law enforcement can seize the private communications of every U.S. service provider's customers, no matter where in the world those customers are located or their data is stored. Under settled extraterritoriality principles, however, only Congress has the prerogative and the institutional competence to decide "whether and when to apply U.S. law to actions occurring abroad." Pet. App. 56a (citing *Benz v. Compania Naviera Hidalgo, S.A.*, 353 U.S. 138, 147 (1957)).

Congress is actively considering how best to accommodate these considerations. Both Houses recently held hearings on proposed reforms. This Court should not short-circuit the legislative process, which is functioning as it should—as both Republican and Democratic Members of Congress agree.

Congress alone has the authority and the institutional competence to craft a new legislative scheme for a world not anticipated in 1986. And it has remedial options simply not available to this Court. As Judge Lynch observed, courts confront an "all-or-nothing choice" in interpreting the current statute: Either local, state, and federal law enforcement may demand *all* communications stored abroad; or they may demand *none*. Pet. App. 69a (Lynch, J., concurring).

In contrast, Congress can craft a comprehensive, nuanced solution. Congress will surely insist on protecting all emails stored on U.S. soil, regardless of where disclosed. But as to emails stored in other countries, Congress might decide to authorize law enforcement to use a warrant to obtain communications

stored abroad if the customer is currently a U.S. resident, if the communications are relevant to specified serious offenses, or if the host foreign country has no mutual legal assistance treaty (MLAT) or other agreement with the United States to facilitate the gathering of evidence. Or Congress could retain territorial limits on warrants while adopting fast-track procedures for bilateral foreign cooperation. Until Congress acts, however, the presumption against extraterritoriality directs that the SCA's silence on its application to communications stored overseas means that it must be given no such reach, as the Court of Appeals correctly held.

Granted, "[a]ll-or-nothing" can be an unsatisfying choice. But the presumption against extraterritoriality addresses precisely this dilemma by directing courts to err on the side of the underinclusive interpretation ("nothing"), not the overinclusive one ("all") that risks projecting U.S. authority abroad in a manner that the political branches never envisioned or intended. *See Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1664 (2013). And if it causes "serious, immediate harms" for the statute to stop at the water's edge, Pet. 30, that is all the more reason to urge Congress to move quickly. But it is no excuse to invite the Court to supplant Congress.

This rule of interpretation is no small formality. It ensures that U.S. courts do not accidentally disrupt the "harmony" between nations that is "particularly needed in today's highly interdependent commercial world." *F. Hoffmann-La Roche Ltd. v. Empagran S.A.*, 542 U.S. 155, 164-65 (2004). The Congress that passed the SCA never considered whether to empower

law enforcement officers to seize private communications stored exclusively in a foreign country. Had it done so (and had it anticipated the reach of the global internet and the advent of cloud computing), it is highly doubtful Congress would have granted the broad powers sought here—certainly not to local and state law enforcement on the same basis as federal agents. This Court should resist the Government's invitation to launch a global free-for-all in which any local constable in any nation where a provider can be found may unilaterally demand private electronic communications stored in any other country, without the host country's knowledge or consent.

In all events, review of this issue now would be premature. The Second Circuit is the only appellate court to have addressed these issues. Other providers are litigating numerous cases—currently pending before courts in at least four circuits—addressing the extraterritorial reach of the SCA. Those cases involve a variety of factual circumstances, including where and how the communications are stored, and how providers retrieve those communications when executing a warrant. The resolution of those cases will sharpen the legal issues and shed light on the broader policy considerations and various factual scenarios the Government invokes in its petition, but which are not presented in the record before this Court. This is the paradigmatic situation in which further percolation is warranted before this Court enters the fray. If Congress has not acted by the time these other cases reach the Court, notwithstanding the current bipartisan momentum, then this Court will have the opportunity to consider afresh the

Government's plea for a judicial rather than legislative revision to the statute.

On the merits, the central issue under this Court's extraterritoriality doctrine is identifying the SCA's focus—and where the conduct relevant to that focus occurs. The Court of Appeals correctly ruled that the *Stored Communications* Act's focus is protecting *communications in storage*. So for purposes of the extraterritoriality analysis, the SCA applies where the communications are stored. And because everyone agrees the statute does not apply abroad, the SCA reaches only communications stored in the United States.

The Government's chief contention is that the statute's focus is instead on *disclosure*. The Government reasons that, because the communications are disclosed to law enforcement in the United States, there is no extraterritorial application of the statute, regardless of where those emails are stored. But the only way the Government can even purport to shift the focus from storage to disclosure is by wrenching the law-enforcement exception out of its statutory context. Section 2703 creates an express exception to the Act's privacy protections for electronic communications held in electronic storage, §§ 2701 and 2702. Protecting those communications "in electronic storage" is the glue that binds these provisions together. *See* Pet. App. 38a-39a. Just as there is no indication that Congress intended §§ 2701 and 2702 to protect the privacy of communications stored in foreign countries (which, like Ireland, may have data protection laws that conflict with our own), there is no indication that § 2703's exception for federal, state, and local

law-enforcement access applies to those foreign-stored communications.

The petition should be denied.

STATEMENT

1. By the mid-1980s, communications had begun migrating from sealed envelopes and landline telephones to the "electronic mail," "videotext," and "paging" services that became state of the art during the Reagan Administration. H.R. Rep. No. 99-647, at 22-23 (1986). Fearing that reliance on these third-party services would "gradually erode" privacy, S. Rep. No. 99-541, at 5 (1986), Congress enacted the Electronic Communications Privacy Act in 1986. Title II of that Act is known as the Stored Communications Act (SCA).

"[T]he first three sections of the SCA," 18 U.S.C. §§ 2701, 2702 & 2703, "contain its major substantive provisions." Pet. App. 38a. Section 2701 protects communications in electronic storage against access by outsiders, prescribing penalties for "intentionally access[ing] without authorization a facility through which an electronic communication service is provided." Section 2702 protects the privacy of stored electronic communications by barring providers from "knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service" without the customer's consent. Finally, § 2703 protects private communications in electronic storage from indiscriminate incursions by *law enforcement*, by providing a limited exception to the restrictions on access to and disclosure of stored

communications. *See* 18 U.S.C. § 2701(c)(3) ("this section does not apply with respect to conduct authorized ... in section 2703"); § 2702(b)(2) (similar). It also imposes heightened procedural requirements for officers to obtain more sensitive information like the content of electronic correspondence. To that end, § 2703 authorizes law-enforcement officers—federal, state, or local, *see* § 2711(4)—to "require the disclosure by a provider of electronic communication service of the contents" of those communications "in electronic storage ... only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction."

2. Microsoft is a global leader in communications and cloud-based computing services. Customers around the world trust Microsoft to securely store their private electronic communications. Those customers range from individual users of its web-based email service (now called Outlook.com) to corporations, government agencies, and other enterprises.

While the notion of "cloud" storage sounds metaphysical, the storage of customers' private communications is quite physical: Each customer's communications reside on an identifiable, physical computer in a specific brick-and-mortar datacenter, which the customer's own computer accesses remotely when she pulls up her email. *See Riley v. California*, 134 S. Ct. 2473, 2491 (2014) ("Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device it-

self."). To provide responsive and reliable service, Microsoft stores its customers' communications in the datacenter closest to each customer's reported residence. Doing so allows Microsoft to improve the quality and speed of its service, because network speed (or "latency") is a function of the distance data travels over physical cables from the datacenter in which it is stored. Pet. App. 7a n.5.

One such datacenter is in Dublin, Ireland. When a customer reports a country of residence for which Dublin is the closest datacenter, Microsoft assigns that customer's account to that datacenter. That means the account's email content—i.e., the message and subject line—is stored on computer servers in Dublin. That content is not stored in any form inside the United States. Pet. App. 7a-8a.

3. a. In 2013, a magistrate judge issued a warrant to search and seize "all e-mails" stored in a specified customer's Microsoft email account and "all ... other information" related to the account (the Warrant). *See* Pet. App. 75a-76a. The Government then served the Warrant on Microsoft and directed the company to "seize" any of the targeted communications within Microsoft's possession and to "produce" them to federal agents. *See* Pet. App. 2a. In response, Microsoft turned over account information stored in the United States, including the customer's address book. But the targeted email content was stored in Dublin. Microsoft therefore moved to vacate the Warrant insofar as the Government invoked § 2703(a) to compel Microsoft's assistance with executing a search warrant in a foreign country.

Microsoft explained that U.S. law enforcement could obtain the communications it sought through the process established by the MLAT between the United States and Ireland. The Government did not dispute that the MLAT process was available to obtain the communications. It simply argued it would be faster to obtain the communications from Microsoft's Dublin datacenter without invoking the MLAT process, and without seeking the consent of the Irish Government.

The magistrate judge denied Microsoft's motion. He analogized the Warrant to a subpoena seeking a company's own business records. Concluding that an SCA warrant should be considered "a hybrid: part search warrant and part subpoena," he ruled that Microsoft must produce the customers' private correspondence in Microsoft's possession or control, even though the communications were stored exclusively in Ireland. Pet App. 84a-85a.

The district court summarily affirmed, and held Microsoft in contempt for refusing to comply with the Warrant. Pet. App. 101a-103a.

b. The Second Circuit reversed unanimously. The court applied the two-step framework for the presumption against extraterritoriality that this Court articulated most recently in *RJR Nabisco*, *Kiobel*, and *Morrison v. National Australia Bank Ltd.*, 561 U.S. 247 (2010). Under that framework, a court asks first whether Congress expressly provided that a statute should apply extraterritorially, and if not, whether the challenged application of the statute is extraterritorial—and therefore unlawful. Applying that rule,

the Court of Appeals concluded that "the District Court lacked authority to enforce the Warrant against Microsoft" because "[n]either explicitly nor implicitly does the statute envision the application of its warrant provisions overseas." Pet. App. 4a, 5a, 22a.

At the first step of the *Morrison* analysis, the court held "with relative ease" that the SCA may not be applied extraterritorially: Congress did not expressly provide for extraterritoriality in the statute. It used the term "warrant," which has historically been understood to be limited to searches and seizures executed in the United States. And there was no indication that the Congress of 1986 had envisioned "a globally-connected Internet available to the ... public for routine e-mail" use. Pet. App. 14a, 23a. The court noted that the Government had "conceded" that "the warrant provisions of the SCA do not contemplate or permit extraterritorial application." Pet. App. 23a-24a.

The dispute therefore turned on *Morrison*'s second step: determining the statute's focus, and whether, in this case, the conduct relevant to that focus would occur domestically or abroad. The court explained that "the relevant provisions of the SCA focus on protecting the privacy of the content of a user's stored ... communications," and because those stored communications are "'the object of the [SCA's] solicitude,'" the location where those communications are stored is the relevant focus. Pet. App. 36a-37a (quoting *Morrison*, 561 U.S. at 267). The Warrant required correspondence to be seized from storage in Dublin. Thus, the court concluded, directing Microsoft to assist with executing the Warrant would entail an impermissible

extraterritorial application of the SCA. Pet. App. 44a-47a.

The Court of Appeals further explained that the magistrate judge had incorrectly relied on corporate subpoena cases. Microsoft is a mere "caretaker" of customers' private email correspondence, unlike "subpoena recipients who are asked to turn over records in which only *they* have a protectable privacy interest." Pet. App. 34a-35a, 44a-45a. The court observed that, consistent with the presumption against extraterritoriality, its interpretation of the SCA avoids the possibility of "conflicts with foreign laws and procedures" that Congress did not clearly authorize—particularly given that § 2703 applies equally to state and local law enforcement. Pet. App. 25a (quoting *EEOC v. Arabian Am. Oil Co.* (*Aramco*), 499 U.S. 244, 256 (1991)); *see* Pet. App. 44a-46a.

Judge Lynch concurred. He found the case "close[]," but nevertheless "c[a]me out in the same place" as the panel opinion because "the better answer" is that Congress never "demonstrated a clear intention to reach situations of this kind in enacting the Act," or even "g[ave] any thought at all to potential transnational applications of the statute." Pet. App. 67a-68a. He explained that "[i]t will often be tempting to attempt to protect American interests by extending the reach of American law and undertaking to regulate conduct that occurs beyond our borders," but "the decision about whether and when to apply U.S. law to actions occurring abroad is a question that is left entirely to Congress." Pet. App. 55a-56a. He therefore "emphasize[d] the need for congressional action to revise a badly outdated statute." Pet. App. 49a.

He also called on "the Justice Department [to] respond to this decision by seeking legislation" to "create nuanced rules" that only Congress, not the courts, could provide. Pet. App. 69a, 71a.

c. The Government petitioned for rehearing en banc. Without calling for a response, the Court of Appeals denied the petition by an evenly divided vote, with three judges recused. Judges Cabranes, Raggi, Droney, and Jacobs each dissented from the denial and joined each other's dissents. Pet. App. 120a-154a. Judge Carney, who authored the panel opinion, responded to their critiques in a concurrence. Pet. App. 107a-119a.

REASONS FOR DENYING CERTIORARI

This Court should deny certiorari for three reasons. *First*, there is rare uniform agreement across all three branches of the federal government, both political parties, and the private sector that Congress must modernize the badly outdated Stored Communications Act. The 99th Congress did not draft a statute that addresses the challenges posed by foreign data privacy laws and global data storage, and only Congress can now rewrite the statute in a way that crafts a comprehensive, balanced solution to those knotty issues. This Court's intervention at this stage could derail the active legislative process that represents the only avenue for a comprehensive update of this outmoded statute. *Second*, the Court of Appeals properly followed this Court's well-established approach to determining when a statute can be read to apply in a foreign country. The longstanding presumption against extraterritoriality

requires courts to defer to precisely the sort of political process that is already under way. The Court of Appeals correctly applied that presumption in holding that, until Congress provides otherwise, the SCA is not properly read to cover communications stored in a foreign country. *Third*, there is no circuit conflict on the question presented, and this Court should, at minimum, decline to take up the question until it has the benefit of further percolation in other courts of appeals, which will soon consider the same question in a variety of other factual contexts.

I. Further Review Is Not Warranted Because Congress Is Actively Considering Amendments To The SCA That Would Expressly Provide For Limited Extra-territorial Reach.

A. The presumption against extraterritoriality ensures that courts do not apply statutes in ways that risk "unintended clashes between our laws and those of other nations." *Aramco*, 499 U.S. at 248. The presumption serves to protect against "international discord," *id.*, by declining to read statutes to intrude on the sovereignty of other nations unless Congress has clearly expressed its intention to reach abroad.

The Congress that enacted the SCA in 1986, before the advent of the global internet, expressed no such intent. Nor did it say anything about compelling service providers to reach into foreign countries to seize private email communications stored there. If domestic law enforcement agencies want that power, even where such access could violate foreign data privacy laws, they must make their case to Congress—

as they are doing right now. That body can then balance law enforcement needs against competing interests, including: our respect for foreign sovereignty (including foreign privacy laws and treaties); the implications for our own nation's sovereignty (and the privacy of our citizens) if other countries reciprocate by requiring providers within their jurisdictions to turn over private emails stored in the United States; and potential harm to the U.S. technology industry.

Congress can craft a far more nuanced solution than the all-or-nothing alternatives presented here. Congress is currently considering several proposals that would do just that. The bipartisan International Communications Privacy Act (ICPA), for example, was introduced by Senators Orrin Hatch and Christopher Coons on July 27, 2017. S. 1671, 115th Cong. (2017). ICPA is precisely the sort of balanced solution that litigation cannot achieve. ICPA would create a clear legal framework under which law enforcement can obtain electronic communications regardless of their location, but only those belonging to certain individuals, including "United States person[s]" and persons "physically located in the United States." S. 1671, 115th Cong. § 102. It also would allow U.S. law enforcement to obtain foreign-stored electronic communications of foreign nationals in specified circumstances. *Id.*

This and other pending efforts to update the SCA illustrate why this Court has developed a robust presumption against extraterritoriality to protect Congress's prerogatives. The presumption "cautions courts to assume that legislators take account of the legitimate sovereign interests of other nations when

they write American laws. It thereby helps the potentially conflicting laws of different nations work together in harmony—a harmony particularly needed in today's highly interdependent commercial world." *F. Hoffmann-La Roche*, 542 U.S. at 164-65.

It is undisputed that the communications at issue here "lie[] within the jurisdiction of a foreign sovereign," and that "Microsoft would have to collect the data from" within the sovereign territory of Ireland in order to comply with the Warrant. Pet. App. 21a, 45a. And all here agree that applying the SCA to reach electronic communications stored abroad has, at a minimum, the *potential* to create just the type of international discord that the presumption against extraterritoriality is intended to prevent. *See, e.g., Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights: Hearing Before the S. Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary* (*May 24 Hearing*) at 50:30-51:40, https://perma.cc/GB66-6CTS (testimony of Brad Wiegmann, Deputy Assistant Att'y Gen., U.S. Dep't of Justice) ("We certainly didn't mean ... to downplay the potential for conflicts when U.S. authorities are seeking data overseas.... The potential for such conflicts certainly exists.").

In fact, it already has. When the magistrate judge ordered Microsoft to seize emails stored in Ireland at the behest of the Government, the European Commissioner for Justice protested: "The effect of the US District Court order is that it bypasses existing formal procedures that are agreed between the EU and the US, such as the Mutual Legal Assistance Agreement, that manage foreign government requests for access

to information and ensure certain safeguards in terms of data protection." CA2 App. 151.[2] She added, "[T]he extraterritorial application of foreign laws (and orders to companies based thereon) may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the Union." *Id.* Members of the European Parliament and the government of Ireland itself subsequently pronounced the execution of the Warrant an incursion into Ireland's sovereign territory. *See* Ireland CA2 Br. at 1 (stating Ireland's "genuine and legitimate interest in potential infringements by other states of its sovereign rights with respect to its jurisdiction over its territory"); Albrecht CA2 Br. at 9 ("[T]he transfer by Microsoft of the content of the email account from Ireland to the United States is not permitted by EU law.").

This international discord will only grow when the European Union's General Data Protection Regulation (GDPR) goes into effect in May 2018. Article 48 of the GDPR restricts when data can be disclosed pursuant to a non-EU court order. It states that "[a]ny judgment of a court ... requiring a [provider] to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement."[3]

---

[2] The Joint Appendix in the Court of Appeals is cited as "CA2 App. __." Amicus briefs filed in the Court of Appeals are cited as "__ CA2 Br.," according to the lead amicus.

[3] The Government speculates (Pet. 32 n.7) that other GDPR provisions may still allow compliance, notwithstanding the clear

B. The Government asserts (Pet. 30-31) that this Court must intervene because a legislative solution is "speculative." But Congress has already begun the process of updating various outdated provisions of the SCA. Earlier this year, for example, the House passed the Email Privacy Act—within a month after it was introduced. H.R. 387, 115th Cong. (2017). That bill would, among other things, amend § 2703(a) to require the Government to obtain a warrant before requiring providers to disclose the content of *all* electronic communications. The bill was recently introduced in the Senate. S. 1654, 115th Cong. (2017).

Similarly, with respect to law enforcement access to data stored abroad, there is broad bipartisan agreement that congressional action is necessary, and that reforms should be enacted swiftly. Indeed, that agreement extends across all three branches of Government:

Legislative Branch. Congress has thoroughly debated the question over a series of hearings, and Members of Congress of both parties have urged prompt action, emphasizing that this is a job for Congress, not courts. *See, e.g.*, Press Release, Sen. Orrin Hatch, Hatch Urges Senators to Support International Communications Privacy Act (Aug. 1, 2017), https://perma.cc/96FP-PXDY ("This is a policy question for Congress.... [I]t is Congress's job to set the bounds of government's investigatory powers. We

---

language of Article 48. But Article 48 is intended to prevent court-ordered transfers that would bypass the MLAT process, and no other provision expressly authorizes a provider to comply with a non-EU warrant seeking data stored in the EU.

decide what government officials can and cannot do. We should not pass the buck to the judiciary merely because this is a complicated issue."); Press Release, Second Circuit Ruling Gives Data Privacy Bill Momentum in Congress (July 14, 2016), https://perma.cc/BF49-N2YE (statement of Rep. Tom Marino) ("It is Congress' job to recognize these lapses and update our laws to reflect the issues of the day. Today's ruling clearly calls for Congress to act."); *id.* (statement of Rep. Suzan DelBene) ("Our electronic communications laws never contemplated this era of cloud storage .... *It is the job of Congress to bring the law up to date where clear gaps exist.*" (emphasis added)).

Executive Branch. As noted, the Government itself has recognized "the need for a legislative fix" and is actively encouraging Congress to "act swiftly" to enact reforms. *See May 24 Hearing*, https://perma.cc/GB66-6CTS (written statement of Brad Wiegmann) 2, 8; *see id.* at 9 ("[A] legislative solution [should] protect[] public safety and national security, allow[] U.S. industry to compete globally, and provide[] a clear set of rules to guide access to data by both domestic law enforcement and our international partners."). Its proposal is linked with a broadly supported measure to facilitate data sharing between the United States and the United Kingdom—a measure that gained additional momentum in the wake of the May 2017 terrorist attack in Manchester, England. *See May 24 Hearing* at 14:30-16:10 (comment of Sen. Lindsey Graham).

Judicial Branch. Every court of appeals judge to have considered the issue (regardless of their ultimate views on the question presented) has also

agreed that the statute must be updated. Judge Lynch noted, for example, that "the statute should be revised, with a view to maintaining and strengthening [its] privacy protections, rationalizing and modernizing the provisions permitting law enforcement access to stored electronic communications and other data where compelling interests warrant it, and clarifying the international reach of those provisions after carefully balancing the needs of law enforcement ... against the interests of other sovereign nations." Pet. App. 71a-72a (Lynch, J., concurring).

As Judge Carney explained, "we can expect that a statute designed afresh to address today's data realities would take an approach different from the SCA's, and would be cognizant of the mobility of data and the varying privacy regimes of concerned sovereigns, as well as the potentially conflicting obligations placed on global service providers." Pet. App. 118a (Carney, J., concurring in the denial of rehearing en banc). Likewise, Judge Jacobs (speaking for the four dissenters) stated that, "I too would like to see Congress act, chiefly to consider certain ramifications, such as whether the United States might be vulnerable to reciprocal claims of access through local offices of American companies abroad." Pet. App. 123a (Jacobs, J., dissenting from denial of rehearing en banc).

C. Legislative reform efforts have vigorous support from the private sector. The nation's major technology companies, including Microsoft, Apple, Facebook, and Google recently voiced their support

for ICPA.[4] Industry groups, including the U.S. Chamber of Commerce, the National Association of Manufacturers, and the Software and Information Industry Association similarly support legislative reform.[5]

Indeed, what is most likely to stall this steady march toward bipartisan congressional action is this Court's intervention. Senator Coons, for example, recently cautioned the Justice Department that "it would raise questions ... about how committed you are about seeking a resolution through Congress if you are also seeking a judicial remedy at the same time." *May 24 Hearing* at 57:15-57:30 (statement of Sen. Christopher Coons). And Senator Hatch, reacting to the petition here, chided: "I'm disappointed by the Department's decision to seek Supreme Court review of the Microsoft warrant case.... [ICPA] would create a workable, modern framework for law enforcement access to electronic communications." Press Release, Sen. Orrin Hatch, Hatch Statement on DOJ Decision to Seek Review in Microsoft Warrant Case (June 26, 2017), https://perma.cc/QRG4-4NBH.

This Court should decline the Government's invitation to disrupt the ongoing legislative process.

D. The Government's own petition further illustrates why the appropriate recourse is to Congress, not this Court. Swaths of the petition present policy

---

[4] Letter from technology companies to Sens. Orrin Hatch, Christopher Coons, and Dean Heller, https://perma.cc/KCN9-XJ64.

[5] Letter from industry groups to Sens. Orrin Hatch and Christopher Coons (July 27, 2017), https://perma.cc/6482-3Z93.

arguments for why law enforcement *should* be permitted to compel service providers to import private communications from a foreign country without the knowledge or consent of that country, not why the Congress that enacted the SCA in 1986 *already provided* that power. *See* Pet. 26-33.

But whether the SCA should be extended in whole or in part to communications stored in a foreign country is "manifestly ... not" for the courts to decide, but for Congress alone. Pet. App. 69a (Lynch, J. concurring). That is why the "policy concerns raised by the government ... require the attention of Congress"—the branch that can "balanc[e] the needs of law enforcement ... against the interests of other sovereign nations." Pet. App. 68a-69a, 72a (Lynch, J., concurring). The Government recognizes that "courts should avoid 'judicial-speculation-made-law—divining what Congress would have wanted if it had thought of the situation before the court.'" Pet. 21 (quoting *Morrison*, 561 U.S. at 261). Yet that is exactly what the Government asks this Court to do.

The Government asserts that other providers have relied on the opinion below in a manner that hampers law-enforcement investigations. Pet. 13, 27-29. Google, for example, has invoked the presumption against extraterritoriality in objecting to SCA warrants, even when it cannot identify a specific foreign country where the communications are stored or even say conclusively they were not stored in the

United States during the relevant period of time.[6] That scenario may present different policy and legal issues. The record here, however, describes only Microsoft's particular architecture and reveals nothing about how other providers operate or respond to search warrants. Nor did the Second Circuit pass upon the issues the Government raises regarding Google's practices. Congress, by contrast, is not "limited by ... the information provided by litigants in a particular case," Pet. App. 70a (Lynch, J., concurring), and can craft a solution that accounts for the range of network designs used by different players in the U.S. technology industry.

E. The Government's policy arguments illustrate why these issues are properly the province of Congress. The Government asserts that the Second Circuit's refusal to grant law-enforcement officers the unilateral power to reach into a foreign country to access private communications stored there could hamper law-enforcement efforts. Congress will no doubt consider that claim when enacting legislative reform. But there are several countervailing considerations that Congress also must weigh.

First, U.S. citizens' privacy interests are very much at risk: Extending the SCA to authorize wide-ranging international warrants invites foreign nations to reciprocate by likewise demanding that

---

[6] *See In re Search Warrant No. 16-960-M-01 to Google*, 232 F. Supp. 3d 708, 724-25 (E.D. Pa. 2017); *see also, e.g., In re Search of Info. Associated with [redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc.*, No. 16-MJ-00757, 2017 WL 3445634, at *2 (D.D.C. July 31, 2017).

providers copy and transmit to a foreign sovereign the private communications of U.S. citizens stored in the United States, without regard for U.S. law and without the knowledge or consent of the U.S. Government. As Judge Lynch explained, the risk in allowing every country to unilaterally extract private electronic correspondence from every other country is "most easily appreciated if we consider the likely American reaction if France or Ireland or Saudi Arabia or Russia proclaimed its right" to do the same to us. Pet. App. 56a (Lynch, J. concurring).

Second, extending the SCA to reach communications stored in other nations would derogate those nations' sovereignty by allowing federal, state, and local law enforcement to bypass the carefully calibrated, comity-protective framework established through MLATs and other bilateral or multilateral agreements.[7] Congress will certainly weigh the risk of sowing international discord before extending to state and local law enforcement agencies the power to reach

---

[7] The Government is free to convey to Congress its complaint (Pet. 29-30) that the MLAT process is less convenient than requiring a provider to execute an SCA warrant. But for present purposes, the evidence in this case, including a sworn declaration from the former Irish Attorney General, establishes that Ireland, for example, has implemented its MLAT obligations with "highly effective" legislation that is "efficient and well-functioning"; that "urgent requests can be processed in a matter of days"; and that law enforcement may call a hotline on a "24/7" "around-the-clock" basis," to ensure the immediate preservation of data. CA2 App. 115-16, 259-63. If the Government believes that inefficiencies in the MLAT process are relevant to the extraterritoriality analysis, it should develop a record on that in a pending case, rather than attempting to inject extra-record assertions here.

into foreign sovereign territory—which the Government's interpretation of the current statute would allow. State governments are plainly eager to exercise that power, as their brief to this Court demonstrates. But it is for Congress to decide whether law enforcement can reach into foreign countries, and, if so, whether any such power should be restricted to the federal government, which is more likely to give due consideration to potential foreign relations consequences than are state and local governments.

Third, granting the power the Government claims would adversely affect U.S. technology companies. The Government has acknowledged the potential for conflicts with foreign data-privacy laws when U.S. authorities seek to compel providers to access and export communications stored in a foreign country. These conflicts can place U.S. companies in the untenable position of being forced to violate foreign privacy laws to comply with U.S. warrants. And the growing privacy concerns of customers around the world mean that granting U.S. law-enforcement agencies that broad authority would hamstring U.S. companies' ability to compete in the multi-billion dollar cloud-computing industry. *See generally*, BSA | The Software Alliance CA2 Br. While the Government may scoff at technology companies' "business interests" and consideration of their "bottom line[s]," Pet. 32, Congress may take a different view.

Only Congress can balance these interests against those of law enforcement, and it properly falls to Congress to decide whether to authorize such foreign seizures of private data.

F. The Government argues (Pet. 30-31) that it cannot await legislative action—that this Court must intervene immediately because the decision below hinders law enforcement's investigative capabilities. But the Government does not deny that it can secure most of what it needs through MLATs and other bilateral agreements—as it could have long ago in this case. Moreover, Congress likely will resolve the issue before this Court can weigh in. Microsoft has long supported an updating of the SCA, and today the technology industry, consumer groups, and congressional leaders all agree that such an updating is clearly needed and can be achieved only through legislation. Given that broad agreement, and the Government's claims of law enforcement and national security exigency, there is every reason to expect quick action.

II. The Court Of Appeals' Decision Is Correct And Fully Consistent With This Court's Extraterritoriality Precedents.

A. The Second Circuit carefully followed and properly applied this Court's established extraterritoriality analysis set forth in *Morrison*, *Kiobel*, and *RJR Nabisco* to hold that the Warrant would entail an impermissible extraterritorial application of the SCA.

Everyone here agrees about *Morrison*'s first step: The SCA gives no "clear, affirmative indication that it applies extraterritorially." *RJR Nabisco*, 136 S. Ct. at 2101; *see* Pet. App. 23a-24a. The whole case therefore centers on *Morrison*'s second step: What is the "conduct relevant to the statute's focus"—i.e., "the objects of the statute's solicitude"? *RJR Nabisco*, 136 S. Ct. at

2101; *Morrison*, 561 U.S. at 267. If the relevant conduct in this case occurs overseas, then the application of the statute is impermissibly extraterritorial.

The Court of Appeals correctly held that the objects of the *Stored Communications* Act's solicitude are the *stored communications* that the statute protects, and so what matters is where the communications are stored. Pet. App. 38a. As other circuits have recognized, "the [SCA] was born from congressional recognition" of the need to protect "against potential intrusions on individual privacy arising from illicit *access* to ... large data banks that stored e-mails." *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 145 (3d Cir. 2015) (emphasis added and internal quotation marks omitted), *cert. denied*, 137 S. Ct. 36 (2016); *see also, e.g.*, *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072-73 (9th Cir. 2004) ("Just as trespass protects those who rent space from a commercial storage facility to hold sensitive documents, the [SCA] protects users whose electronic communications are in electronic storage with an ISP." (citation omitted)). Indeed, the Government has elsewhere recognized that the SCA's chief object is to "protect[] the privacy of the contents of files stored by service providers."[8]

To accomplish this goal, the SCA's three substantive provisions fit together to regulate the privacy of stored communications. Section 2701 restricts access

---

[8] U.S. Dep't of Justice, Office of Justice Programs, Bureau of Justice Assistance, *Electronic Communications Privacy Act of 1986*, Justice Information Sharing, https://perma.cc/S5NA-WZTB.

to stored communications. It bars a form of hacking: "access[ing] without authorization a facility through which an electronic communication service is provided," to "obtain[]" an "electronic communication ... in electronic storage." Next, § 2702 turns its attention to providers, broadly restricting them from "divulg[ing] ... the contents of a communication while in electronic storage" to anyone not authorized by the customer who entrusted the provider with her personal correspondence. The statute then exempts specified access to and disclosure of communications, including those required by valid law-enforcement demands for "communication[s] ... in electronic storage." § 2703(a). It does so as an express exception to the protections in §§ 2701 and 2702. *See* § 2701(c)(3) ("[T]his section does not apply with respect to conduct authorized ... in section 2703."); § 2702(b)(2) (similar). The "electronic storage" of "communications" is the common object regulated by these interlocking provisions.

The Court of Appeals therefore properly rejected the Government's argument, renewed in its petition, (Pet. 14-16) that the SCA's focus is "disclosure," such that the relevant location is where the communications are disclosed to law enforcement—and not where the communications were stored (and where law enforcement sought to compel Microsoft to access them and copy them out of storage). *See* Pet. App. 37a-41a. That reading of the statute's "focus" requires the reader to isolate § 2703 from the substantive provisions that cross-reference it. It separates the limited law-enforcement exception from the rule. Section 2701, in particular, restricts access to stored communications and does not address "disclosure" or

providers at all. Neither § 2701 nor § 2702 purports to protect communications in electronic storage abroad—and the Government has never suggested they do. Other nations pass their own data privacy laws governing data stored on their own soil. The term "communication ... in electronic storage" cannot have a broader meaning in § 2703's exception than it has in §§ 2701 and 2702's fundamental protections.

Moreover, the Government's construction means that the SCA would not cover conduct that Congress surely intended to cover. Under the Government's construction, the SCA would apply only to circumstances where the disclosure occurs in the United States, but not to circumstances where the disclosure occurs abroad. So, under the Government's construction, § 2702 would not bar a U.S. service provider from disclosing to a foreign tabloid a U.S. citizen's U.S.-stored communications: Enforcing § 2702's ban on disclosure there would be an impermissible extraterritorial application. Yet those are the very communications Congress undoubtedly intended to protect when it enacted the SCA. A much more sensible reading is that the SCA regulates domestic stored communications (wherever disclosed), not domestic disclosures of communications (wherever stored). That is, the SCA's provisions apply only to electronic communications stored here, just as other countries' laws regulate electronic communications stored there.

The Government insists §§ 2701 and 2702 are irrelevant—that the Court of Appeals was required to assess § 2703 in isolation. Pet. 21-22. Statutory construction ordinarily does not work that way—courts routinely recognize the relevance of related

terms in cross-referenced provisions—and this Court has never suggested that the search for the "focus" of a statute eschews context. Quite the opposite: The Court of Appeals' contextual analysis of "focus" tracked this Court's approach in *Morrison*: Just as *Morrison* examined § 10(b) of the Exchange Act in the context of related provisions of the Act, the statute's prologue, and a separate statute enacted by the same Congress, 561 U.S. at 266-69, the Court of Appeals examined § 2703 in the context of the neighboring provisions that expressly cross-reference it—the provisions from which § 2703 creates a limited law-enforcement exception. Pet. App. 36a-41a.

The Government suggests that *RJR Nabisco* overrode *Morrison*'s approach—by requiring, for purposes of *Morrison*'s second step, that a statute's "focus" be analyzed section by section. That is doubly wrong. First, *RJR Nabisco* did not engage in any "provision-specific analysis" in conducting a *focus* inquiry; *RJR Nabisco* never reached *Morrison*'s second step at all, instead resolving the case at step one. *See* 136 S. Ct. at 2103-04; *id.* at 2108-11. Second, even *RJR Nabisco*'s step-one analysis did not involve reviewing each RICO provision in isolation. Rather, it looked to RICO's substantive provisions and private cause of action in "context." *Id.* at 2102, 2106 (internal quotation marks omitted). The Court ultimately held that only certain RICO provisions have extraterritorial application. But this was so, the Court explained, because where there *is* a clear indication that a statute applies extraterritorially, "the presumption ... operates to limit that [extraterritorial application] to its terms." *Id.* at 2102 (quoting *Morrison*, 561 U.S. at 265).

B. The Government's other criticisms of the Court of Appeals' decision are equally meritless. The Government faults the Court of Appeals for supposedly finding that the SCA's focus is "privacy," Pet. 17, and responds that the only conduct relevant to that focus occurs in the United States. But the Court of Appeals did not hold that the SCA's focus is protecting some abstract and generalized privacy interest, whose location would be difficult to pin down. Rather, the court recognized that the SCA's focus is on the private *communications in electronic storage* that the statute protects and regulates, and that exist on identifiable computer servers in identifiable physical locations. Pet. App. 38a-39a.

Given that specific focus, the Court of Appeals correctly identified the relevant conduct under § 2703 as the seizure (via the compelled assistance of the service provider) of the communications from the servers on which the data is securely stored. Because the servers in this case are located in Ireland, that conduct necessarily occurs outside the United States. Pet. App. 43a-44a.

The Government argues that seeking emails stored in Ireland is a wholly domestic application of the SCA, even though the Government would compel Microsoft to search the computer servers in Dublin, identify and access the private communications stored there, copy those communications, and then export them from Ireland into the United States. The Government refers to the accessing and copying of private stored communications in Ireland as the mere "antecedent conduct of gathering responsive mate-

rial." Pet. 18. But what the Government calls "gathering responsive material," Congress expressly termed the "execution of a search warrant." § 2703(g). And execution of a U.S. warrant to seize documents in a foreign country is precisely the kind of foreign incursion that the presumption against extraterritoriality was designed to prohibit, absent clear authorization by Congress.

The Government also errs in suggesting (Pet. 18-19) that the storage location should be irrelevant because Microsoft "chooses" where to store customers' communications (which it does in order to deliver the fastest service to the customer). That is like saying a U.S. company whose shares trade on a foreign exchange should be subject to suit under the Securities Exchange Act, notwithstanding *Morrison*, because the company "chose" to list them there. The presumption against extraterritoriality takes statutes, and businesses, as it finds them. Besides, the Government's interpretation of the SCA would apply equally to a provider that contracted with Irish customers with an express promise to store their communications only in Ireland and never export them. Under the Government's reading, so long as the communications can be accessed from and disclosed in the United States, they can be reached with an SCA warrant.

Nor is it relevant that Microsoft retains the right, in the course of its ordinary operations, to migrate customer emails from one datacenter to another, consistent with the needs of the customer and Microsoft's contractual commitments. *See* Pet. 18. That has no bearing on whether the SCA is being applied extraterritorially when the Government uses a warrant to

conscript Microsoft to seize a customer's private communications from storage in Ireland so they can be exported to the United States and produced to the Government.

Next, the Government invokes *Marc Rich & Co., A.G. v. United States*, 707 F.2d 663 (2d Cir. 1983), and similar cases addressing the cross-border reach of subpoenas of a company's own business records. It suggests that the decision below is "inconsistent with settled law on the operation of subpoenas." Pet. 22-24. This echoes the magistrate judge's view that the term "warrant" in § 2703 actually means a "hybrid ... subpoena." Pet. App. 84a. But § 2703 addresses warrants and subpoenas separately, and the Court of Appeals correctly recognized that different terms in a single statute should be given their respective, ordinary meanings. Pet. App. 30a-36a; *see Mohamad v. Palestinian Auth.*, 132 S. Ct. 1702, 1708 (2012). By rule, and by legal presumption, warrants are limited to U.S. territory—in stark contrast to the manner in which lower courts have treated subpoenas.

In any event, this Court has never embraced the *Marc Rich* rule—that a court may compel a company within its jurisdiction to produce documents in its custody or control, even when the documents are located abroad and their disclosure would violate foreign law. *Marc Rich* and comparable cases arose before *Morrison*. They thus do not address whether compelling such actions in a foreign country would contravene the presumption against extraterritoriality under the *Morrison* rubric. This case, which involves warrants, is not a suitable vehicle for the Court to address that other question about subpoenas. The Government

errs in arguing from a premise that merely assumes the answer to a different extraterritoriality question this Court has never resolved.

Moreover, whatever the vitality of the *Marc Rich* line of cases, they are different. Those cases involved compelled disclosure of a company's own corporate records. From the perspective of incursions on sovereignty, that is far afield from the situation here: The Government is not using the search warrant to compel Microsoft to gather its own documents, but rather to search for and seize private correspondence held in trust for its customers and subject to legal protections in other countries. No court has extended *Marc Rich* to reach a third party's private papers held in another country, even in the context of a subpoena, let alone a law-enforcement search warrant.

Finally, as this Court recognized in *Morrison*, "[t]he probability of incompatibility with the applicable laws of other countries" is a strong signal that Congress did not intend such a foreign application of a statute. 561 U.S. at 269. The Government has itself acknowledged the very real possibility of conflicts when it uses SCA warrants to compel the production of data stored in foreign countries. As documented above (at 16), that probability has already materialized into reality. This is exactly the sort of international strife the presumption against extraterritoriality is supposed to prevent.

III. Because This Is A Question Of First Impression In The Courts Of Appeals, This Court Should Await Further Percolation.

The Government's petition is missing the one most common ingredient of a successful cert. petition: a circuit conflict. This issue is so cutting edge that no other court of appeals has yet considered it. Thus, this Court does not yet have the full benefit of "the crucible of adversarial testing on which [it] usually depend[s]." *Maslenjak v. United States*, 137 S. Ct. 1918, 1931 (2017) (Gorsuch, J., concurring in part and concurring in the judgment).

Beyond the usual value to this Court of considering the perspectives and analyses of multiple circuits, awaiting further appellate decisions is necessary here to allow this Court to better evaluate the variety of factual scenarios in which the question could arise. The Government only reinforces how important that is by citing several magistrate judge decisions involving warrants directed at Google. Google's cloud technology is different from Microsoft's storage architecture. Several magistrate judges (and more recently, three district courts) have noted that Google constantly moves data from location to location, making "it uncertain which foreign country's sovereignty would be implicated," *In re Search Warrant No. 16–960–M–01 to Google* (*In re Search Warrant*), No. 16-1061-M, 2017 WL 471564, at *12 (E.D. Pa. Feb. 3, 2017); *accord, e.g.*, *In re Search of Content Stored at Premises Controlled by Google Inc.*, No. 16-MC-80263, 2017 WL 3478809, at *1 (N.D. Cal. Aug. 14, 2017). Google's practice can make it impossible to say with certainty whether the data is in fact located outside

the United States. *See In re Search Warrant*, 2017 WL 471564, at *13. Here, by contrast, the record reflects that the private communications the Government seeks are stored in a discrete, identifiable location—a server in a datacenter in Dublin, Ireland, where it is regulated by Irish data protection law and subject to the United States-Ireland MLAT. No appellate court has grappled with how that difference affects the extraterritoriality analysis.

Similarly, the Government protests that "[t]he decision blocks government access to foreign-stored emails even when the user is a U.S. citizen living in the United States." Pet. 27. But that possibility is not presented here: The record in this case is silent on the residence of the targeted account holder, and the Government has never suggested that the account holder is a U.S. citizen or resides here. Other pending cases can shed light on the extent to which the account holder's residence is relevant to the extraterritoriality analysis—as the Government suggests it is.

In other words, while the Government's complaints here are largely about Google's storage architecture and the possibility that investigations involving U.S. persons will be affected,[9] the record here sheds no light on those considerations. The pend-

[9] The Government contends, for example, that the decision below "provides a roadmap for terrorists and criminals in the United States to insulate electronic communications from U.S. investigators." Pet. 27. But, under current law, a criminal seeking to manipulate data location for purposes of evading U.S. law enforcement would simply use a foreign email service, like mail.ru, that U.S. authorities could not reach at all.

ing cases involving Google and other providers will allow the courts to address the SCA's scope and how the presumption against extraterritoriality applies in a variety of factual contexts, thereby enriching this Court's understanding of both the SCA and how the abstract legal issues presented play out in the real world. The ultimate appellate rulings on those matters will give this Court the benefit of the wisdom and perspectives of courts addressing whether and how the SCA applies to an array of technologies.

Thus, even if the Court is inclined to take up the question at some point, its ultimate review would benefit from following its usual practice of waiting and allowing further evaluation by the appellate courts.

CONCLUSION

The petition for a writ of certiorari should be denied.

Respectfully submitted,

Bradford L. Smith
David M. Howard
John Frank
Jonathan Palmer
Nathaniel Jones
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052

James M. Garland
Alexander A. Berengaut
COVINGTON & BURLING LLP
850 10th Street, NW
Washington, DC 20001

E. Joshua Rosenkranz
Counsel of Record
Robert M. Loeb
Brian P. Goldman
Evan M. Rose
Hannah Garden-Monheit
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019
(212) 506-5000
jrosenkranz@orrick.com

August 28, 2017